

Ship every season.

ERP and e-commerce security, IP protection, SOC, privacy and supplier assurance for textiles, apparel and consumer manufacturing.

Three questions every exporter and brand should answer

If ERP went dark tonight, would this week's shipment sail?

Mapping what packing, invoicing and export documents depend on, and testing backups, decides whether ransomware costs a day or a season.

Could a fake email move our export proceeds?

Business email compromise targets merchandisers and buyers' payment cycles; verification procedures and mailbox controls stop it.

Who can still download our designs?

Contractors, leavers and shared cloud folders are the most common paths for tech packs and costings to leave.

35.5 mn

Consumers in VF Corp's
2023 incident

US\$100 m

Hanesbrands' one-
quarter sales hit

45 mn+

Directly employed in
Indian textiles

6 hours

Incident reporting to
CERT-In

Built for every manufacturer and brand

Spinning and weaving mills · processing and job-work units · garment and home textile exporters · footwear manufacturers · consumer products manufacturers · brand owners and licensees · D2C and e-commerce arms.

The rules that drive your security calendar

Instrument	Key cybersecurity expectations
CERT-In Directions · audit guidelines (2022, 2025)	6-hour reporting, 180-day logs; independent audits
SEBI LODR · DPDP	Quarterly incident disclosure (listed); consumer and worker data
Buyer, tax and product rules	Brand questionnaires; GST e-invoicing; BIS QCOs; PCI DSS; EU CRA

WHAT WE DO

ERP, e-commerce, IP, SOC, privacy and suppliers

ERP & E-commerce Security

ERP, PLM, D2C site, app, buyer portal and marketplace integration testing.

IP Protection

Classification, DLP, contractor and leaver controls, forensic readiness.

24/7 SOC

Plant, office and cloud monitoring; account takeover, BEC and fraud detection.

Privacy & DPDP

Consumer, loyalty, employee and worker data programme and breach workflows.

Supplier Assurance

Job-worker and supplier assessments, contract clauses, joint exercises.

Buyer Questionnaire Readiness

ISO 27001 and PCI DSS readiness; reusable evidence packs for brands.

Choose your starting point

Foundation

IT and plant assessment, backup and recovery review, email and BEC controls, policy and questionnaire pack. For mills, job-workers and single factories.

Assurance

ERP, PLM and portal testing, IP protection programme, annual audit, 24x7 SOC. For exporters and multi-unit manufacturers.

Continuous Resilience

Continuous web, API and app testing, supplier assurance, SOC with fraud and brand monitoring, DPDP and Board reporting. For brand owners, listed groups and D2C businesses.

Why Codec Networks

CERT-In empanelled

for information security auditing services, and empanelled with NISCI for application audit services.

Certified

ISO 9001:2015, ISO/IEC 27001:2022 and ISO/IEC 20000-1:2018.

Regulation-mapped

Every finding mapped to ISO/IEC 27001, PCI DSS, CERT-In and DPDP expectations and your buyers' security questionnaires.

One connected partner

Testing, audits, SOC, forensics and privacy linked from finding to closure.

Book a scoping session

Share your units, systems, buyers, suppliers and channels. We will propose a practical, season-aware assessment and assurance plan.

New Delhi: 507, 5th Floor, New Delhi House, Barakhamba Road, Connaught Place – 110001

Gurugram: 707, 7th Floor, Silverton Tower, Golf Course Extension Road, Sector 50 – 122018

Call: 011 430 496 96 · +91 99716 76124 · +91 88007 88220

Email: mktg@codecnetworks.com · www.codecnetworks.com

Regulatory references reflect public instruments as of October 2026; applicability depends on each entity's licence, category and activities. Services support risk reduction and assurance and do not guarantee prevention of all incidents or regulatory compliance. Sources: VF Corporation Form 8-K/A (2024), Hanesbrands Q2 2022 results, Ministry of Textiles, CERT-In. Confirm obligations against the official instruments.